# On a distribution property of the residual order of $a$(mod $p$) (IV) (Analytic Number Theory and Surrounding Areas)

AUTHOR(S):

Chinen, Koji; Murata, Leo

CITATION:

Chinen, Koji ...[et al]. On a distribution property of the residual order of $a$(mod $p$) (IV) (Analytic Number Theory and Surrounding Areas). 数理解析研究所講究録 2004, 1384: 169-174

ISSUE DATE:

2004-07

URL:

http://hdl.handle.net/2433/25747

数理解析研究所講究録 1384 巻 2004 年 169-174



# On a distribution property of the residual order of $a \pmod p$ — IV

大阪工業大学 工学部 知念 宏司 (Koji Chinen)
Department of Mathematics, Faculty of Engineering,
Osaka Institute of Technology.
明治学院大学 経済学部 村田 玲音 (Leo Murata)
Department of Mathematics, Faculty of Economics,
Meijigakuin University.

## 1 Introduction

Let $a$ $(\geq 2)$ be a natural number which is not a perfect $b$-th power with $b \geq 2$. For a prime $p$ not dividing $a$, we define the number

$$D_a(p) = \sharp\langle a \pmod p\rangle$$
$$\text{(the order of the class } a \pmod p \text{ in } (\mathbf{Z}/p\mathbf{Z})^\times)$$

and consider the set

$$Q_a(x;k,l) = \{p \leq x\ ;\ D_a(p) \equiv l \pmod k\}$$

for arbitrary prescribed integers $k$ and $l$. We denote the natural density of $Q_a(x;k,l)$ by $\Delta_a(k,l)$. To be precise, let

$$\Delta_a(k,l) = \lim_{x\to\infty} \frac{Q_a(x;k,l)}{\pi(x)},$$

where $\pi(x)$ means the number of primes not exceeding $x$.

In our papers [2] and [9], we considered the case $k = 4$ (See also [1], [4] and [5]). In these papers, we proved under GRH (=Generalized Riemann Hypothesis), the existence of the natural density $\Delta_a(4,l)$ for $l = 0,1,2,3$ and obtained the explicit values of them. Later in [6] and [10], we extended the result to the cases $(k,l) = (q^i, j)$ and $(k,l) = (5,h)$ respectively, where $q$ is an odd prime, $i \geq 2$, $q|j$ and $1 \leq h < 5$.

In this article, we consider the most general case, i.e. $k$ and $l$ are arbitrary integers. We will show two different types of statements according to the value of $k$:

1° The case $k$ is a prime power: $k = q^i$ $(i \geq 1)$,

2° The case $k$ is a composite number other than 1°.

In both cases, we assume GRH. Then for the case 1°, we can give an explicit formula expressing $\Delta_a(q^i,l)$ for any $l$ (see Theorems 2.1 and 2.2). For the case 2°, we have an algorithm by which we can calculate $\Delta_a(k,l)$ for any $k$ and $l$ effectively (see Section 3).

For our motivation of considering this problem, the reader is referred to [2] or [4]. For some related problems, see [5] or Odoni [11]. The reader who wants to see examples of computer experiments is referred to any of our previously published articles other than [1].

## 2 The case $k$ is a prime power

In this section we consider the case $k = q^i$ ($q$ is a prime number) and $0 \leq l \leq q^i - 1$ ([3] and [6]). First we assume $i \geq 2$ if $q$ is an odd prime, and $i \geq 3$ if $q = 2$. Then in most cases, we have a certain recurrence formula between $\Delta_a(q^i, l)$ and $\Delta_a(q^{i-1}, l)$ which shows a kind of "local equi-distribution property":

**Theorem 2.1** *We assume GRH. Then the density $\Delta_a(q^i, l)$ always exists and we have the following:*

*(I) We have $\Delta_a(8,2) = \Delta_a(4,3)$, $\Delta_a(8,6) = \Delta_a(4,1)$, and $\Delta_a(8,l) = \frac{1}{2}\Delta_a(4,l)$ unless $l = 2, 6$.*

*(II) (Local equi-distribution property) We suppose $i \geq 2$ when $q$ is an odd prime, and $i \geq 4$ when $q = 2$. Then for an arbitrary $l$, we have the relation*

$$\Delta_a(q^i, l) = \frac{1}{q}\Delta_a(q^{i-1}, l).$$

Part (II) of the above theorem tells us that $\Delta_a(q^{i-1}, l)$ is *equally* divided into $q$ values $\Delta_a(q^i, l')$ ($l' = l + iq^{r-1}$, $0 \leq i \leq q-1$). We call it "local equi-distribution property". The former two equalities in Part (I) seem a little mysterious and we do not know so far a heuristic explanation for them.

By Theorem 2.1, the calculation of $\Delta_a(q^i, l)$ is reduced to the case $k = 4$ if $q = 2$ (which is already done in [2] and [9]), and to the case $k = q$ if $q$ is an odd prime. We state the result for $k = q$. Let $a_1$ be the square free part of $a$, $G = \mathbf{Z}/q\mathbf{Z}^\times$ and let $\hat{G}$ be the character group of $G$. We denote the Legendre symbol by $(\frac{\cdot}{q})$ and we define for each $\chi \in \hat{G}$, an absolute constant $C_\chi$ by

$$C_\chi = \prod_{\substack{p:\text{prime} \\ p \neq q}} \frac{p^3 - p^2 - p + \chi(p)}{(p-1)(p^2 - \chi(p))}.$$

Moreover we define

$$\eta_{\chi,a} = \begin{cases} 1, & \text{if } a_1 \equiv 1 \pmod 4, \\ \dfrac{\chi(2)^2}{16}, & \text{if } a_1 \equiv 2 \pmod 4, \\ \dfrac{\chi(2)}{4}, & \text{if } a_1 \equiv 3 \pmod 4. \end{cases}$$

**Theorem 2.2** *Let $q$ be an odd prime, $1 \leq h \leq q-1$, and we assume GRH.*

*(I) If $q \nmid a_1$, then*

$$\Delta_a(q,h) = \frac{q^2}{(q-1)(q^2-1)} - \frac{1}{(q-1)^2}\sum_{\chi\in\hat{G}} C_\chi \chi(-h)\left(1+\eta_{\chi,a}\prod_{p|2a_1}\frac{p(\chi(p)-1)}{p^3-p^2-p+\chi(p)}\right).$$

*(II) If $q|a_1$, then*

$$\Delta_a(q,h) = \frac{q^2}{(q-1)(q^2-1)}$$
$$-\frac{1}{(q-1)^2}\Big[\sum_{\chi\in\hat{G}} C_\chi\Big\{\chi(-h) - \Big(\chi(-h)+2\sum_r \chi(r)^{-1}\Big)\eta_{\chi,a}\prod_{p|2\underline{a_1}}\frac{p(\chi(p)-1)}{p^3-p^2-p+\chi(p)}\Big\}\Big],$$

*where $\sum_r$ means a sum over all $r$ $(1 \le r \le q-1)$ such that $(\frac{hr+1}{q}) = 1$ and $\underline{a_1}$ is the $q$-free part of $a_1$ (i.e. $\underline{a_1} = a_1/q$).*

When $q \ge 5$, the constant $C_\chi$ is not always a real number. For example, when $q = 5$, we have

$$C_{\chi_0} = 1, \qquad C_{\chi_1} = \prod_{p\equiv 2,3 (\mathrm{mod}\, 5)}\left(1-\frac{2p}{(p-1)(p^2+1)}\right) \approx 0.1293079,$$

$$C_{\chi_2} = \prod_{p\equiv 2(\mathrm{mod}\,5)}\left(1+\frac{(p(i-1))}{(p-1)(p^2-i)}\right)\prod_{p\equiv 3(\mathrm{mod}\,5)}\left(1-\frac{(p(i+1))}{(p-1)(p^2+i)}\right)$$
$$\cdot \prod_{p\equiv 4(\mathrm{mod}\,5)}\left(1-\frac{2p}{(p-1)(p^2+1)}\right) \approx 0.3640896 + 0.2240411i$$

and $C_{\chi_3} = \overline{C_{\chi_2}}$, where $\hat{G} = \{\chi_0, \chi_1, \chi_2, \chi_3\}$, $\chi_0$ is principal and $\chi_1^2 = \chi_0$. It is an interesting phenomenon that the cancellation of the imaginary parts of $C_\chi$'s results in real densities, and this can be explained by the use of the Dirichlet characters, similar to the proof of the theorem of arithmetic progressions. From this point of view, the case $k = 4$ is rather special because we do not need imaginary numbers to express the values of characters mod 4 (note that the constant $C$ in [1] or [9] coincides with $C_\chi$ with $\chi$ replaced by the non-principal character mod 4).

Let us see the idea of proof. The special case $l = 0$ is obtained along the same line as in Hasse [7], [8] and Odoni [11]. Indeed, when $q$ is an odd prime (the case $q = 2$ is complicated and omitted),

$$\Delta_a(q^i, 0) = \frac{q}{q^{i-2}(q^2-1)}$$

(the case $i = 1$ is already obtained by Hasse and Odoni). So we are interested in the set $Q_a(x; q^i, l)$ with $1 \le l \le q^i - 1$, we put $l = hq^e$ with $q \nmid h$ and $0 \le e \le i-1$. For $1 \le r < q^i$ $(q \nmid r)$ and $j \ge 0$, let

$$k = \{(\overline{h}r) \pmod{q^{i-e}} + jq^{i-e}\}q^{f-e}$$

where $h\overline{h} \equiv 1 \pmod{q^{i-e}}$, and $(\overline{h}r) \pmod{q^{i-e}}$ means the least natural number which is congruent to $\overline{h}r$ modulo $q^{i-e}$. And let

$$k_0 = \prod_{\substack{p|k \\ p:\text{prime}}} p \quad (\text{the core of } k).$$

The following lemma is the starting point:

**Lemma 2.3** *Let $I_a(p) = |(\mathbf{Z}/p\mathbf{Z})^\times : \langle a \pmod p \rangle|$, the residual index mod $p$ of $a$. Then,*

$$\sharp Q_a(x; q^i, hq^e) = \sum_{\substack{1 \le r < q^i \\ q \nmid r}} \sum_{f \ge e} \sum_{j \ge 0} \sharp \left\{ p \le x \ ; \ I_a(p) = k, \ p \equiv 1 + rq^f \pmod{q^{f+i}} \right\}.$$

This lemma and a similar reasoning to that of [2] allows us to prove the existence of the density $\Delta_a(q^i, l)$ and its expression in infinite series (Theorem 2.4 below). To state the theorem, we need some more notations. We define the following two types of number fields:

$$\begin{aligned} G_{k,n,d} &= \mathbf{Q}(a^{1/kn}, \zeta_{kd}, \zeta_n), \\ \tilde{G}_{k,n,d} &= G_{k,n,d}(\zeta_{q^{f+i}}). \end{aligned}$$

We take an automorphism $\sigma_r \in \mathrm{Gal}(\mathbf{Q}(\zeta_{q^{f+i}})/\mathbf{Q})$ determined uniquely by the condition $\sigma_r : \zeta_{q^{f+i}} \mapsto \zeta_{q^{f+i}}^{1+rq^f}$ $(1 \le r < q^i, \ q \nmid r)$, and we consider an automorphism $\sigma_r^* \in \mathrm{Gal}(\tilde{G}_{k,n,d}/G_{k,n,d})$ which satisfies $\sigma_r^*|_{\mathbf{Q}(\zeta_{q^{f+i}})} = \sigma_r$. We can verify that such a $\sigma_r^*$ is unique if it exists (see [2, Lemma 4.3]). Then we have

**Theorem 2.4** *Under GRH, we have*

$$\sharp Q_a(x; q^i, hq^e) = \Delta_a(q^i, hq^e) \operatorname{li} x + O\left( \frac{x}{\log x \log\log x} \right)$$

*as $x \to \infty$, where*

$$\Delta_a(q^i, hq^e) = \sum_{\substack{1 \le r < q^i \\ q \nmid r}} \sum_{f \ge e} \sum_{l \ge 0} \frac{k_0}{\varphi(k_0)} \sum_{d|k_0} \frac{\mu(d)}{d} \sum_{n=1}^{\infty} \frac{\mu(n) c_r(k,n,d)}{[\tilde{G}_{k,n,d} : \mathbf{Q}]} \tag{2.1}$$

*and*

$$c_r(k,n,d) = \begin{cases} 1, & \text{if } \sigma_r^* \text{ exists,} \\ 0, & \text{otherwise.} \end{cases}$$

*The series in the right hand side of (2.1) always converge.*

We must determine the coefficients $c_r(k,n,d)$ (done in [3, Section 3]). Then Theorem 2.2 is obtained by transforming the series (2.1) into an expression involving some Euler products. Theorem 2.1 is obtained a little easier, but requires a variety of other techniques.

# 3 The case $k$ is an arbitrary composite number

In this section we consider the case $k$ is an arbitrary composite number, especially $k$ has at least two distinct prime factors. The main result for this case is the following:

**Theorem 3.1** *We assume GRH. Then, for any residue class $l \pmod k$, the natural density $\Delta_a(k,l)$ exists and the value of $\Delta_a(k,l)$ is effectively computable.*

We sketch the idea of proof. Let $k = \prod_{i=1}^{r} p_i^{e_i}$ (factorization into prime factors) and we put $l = h\prod_{i=1}^{r} p_i^{f_i}$ $((h,k)=1)$. First we consider the case where $l$ satisfies the condition $p_i^{e_i} \nmid l$ for any $i$, $1 \le i \le r$. Then like Lemma 2.3, we can decompose the set $Q_a(x;k,l)$ as follows:

**Lemma 3.2** *Under the above notations, we have*

$$\sharp Q_a(x;k,l) = \sum_{g_1 \ge f_1} \cdots \sum_{g_r \ge f_r} \sum_{\substack{0<s<k \\ (s,k)=1}} \sum_{t \ge 0} \sharp\Big\{p \le x \ ; \ I_a(p) = m, \ p \equiv 1 + s\prod_{i=1}^{r} p_i^{g_i} \pmod{\prod_{i=1}^{r} p_i^{e_i+g_i}}\Big\},$$

*where*

$$m = \Big\{\bar{h}s \pmod{\prod_{i=1}^{r} p_i^{e_i-f_i}} + t\prod_{i=1}^{r} p_i^{e_i-f_i}\Big\}\prod_{i=1}^{r} p_i^{g_i-f_i}$$

*and* $\bar{h}h \equiv 1 \pmod{\prod_{i=1}^{r} p_i^{e_i-f_i}}$.

Using this lemma, we can prove the existence of the density $\Delta_a(k,l)$ by deducing a similar result to Theorem 2.4, and can find the exact value of it in a similar method to that of [2].

When $p_i^{e_i} | l$ for some $i$, we must appeal to a different method because the decomposition in Lemma 3.2 does not hold. The technique we employ is rather elementary. We construct a certain system of linear equations including $\Delta_a(k,l)$, and show that the solution is unique. We illustrate the idea by an example:

**Example 3.3** $k = 12 = 2^2 \cdot 3^1$. We can know $\Delta_a(12,0)$ unconditionally (similar to [11]). For such an $l$ with $2^2 \nmid l$ and $3 \nmid l$, we can calculate the exact densities

$$\Delta_a(12,1),\ \Delta_a(12,2),\ \Delta_a(12,5),\ \Delta_a(12,7),\ \Delta_a(12,10),\ \Delta_a(12,11).$$

For remaining values of $l$, i.e. $l = 3,4,6,8,9$, we construct a system of linear equations (the underlined values are the remaining densities):

$$\begin{aligned}
\Delta_a(3,1) &= \Delta_a(12,1) + \underline{\Delta_a(12,4)} + \Delta_a(12,7) + \Delta_a(12,10),\\
\Delta_a(3,2) &= \Delta_a(12,2) + \Delta_a(12,5) + \underline{\Delta_a(12,8)} + \Delta_a(12,11),\\
\Delta_a(4,1) &= \Delta_a(12,1) + \Delta_a(12,5) + \underline{\Delta_a(12,9)},\\
\Delta_a(4,2) &= \Delta_a(12,2) + \underline{\Delta_a(12,6)} + \Delta_a(12,10),\\
\Delta_a(4,3) &= \underline{\Delta_a(12,3)} + \Delta_a(12,7) + \Delta_a(12,11).
\end{aligned}$$

We know all the values in the left hand sides by our previous results. In the right hand sides, we can calculate all values which are not underlined by the discussion above. So each equation contains only one undecided value, and we can get it by solving the equation.

The case $k = 12$ is the simplest case, but we can show that we can always construct such a "good" system of equations and can determine any $\Delta_a(k, l)$.

# References


[1] Chinen, K. and Murata, L. : On a distribution property of the residual order of $a \pmod p$, Proc. Japan Acad. **79** Ser. A (2003), 28-32.

[2] _____ : On a distribution property of the residual order of $a \pmod p$, to appear in J. Number Theory.

[3] _____ : On a distribution property of the residual order of $a \pmod p$ — III, preprint.

[4] _____ : On a distribution property of the residual order of $a \pmod p$ (in Japanese) in *Analytic Number Theory — Expectations for the 21st Century —*, RIMS Kokyuroku **1219** (2001), 245-255.

[5] _____ : On a distribution property of the residual order of $a \pmod p$ (in Japanese) in Proceedings of the Conference *AC2001* (Algebra and Computation) held at the Tokyo Metropolitan Univ. (2001), published electronically in ftp://tnt.math.metro-u.ac.jp/pub/ac/2001.

[6] _____ : On a distribution property of the residual order of $a \pmod p$, II (in Japanese) in *New Aspects of Analytic Number Theory*, RIMS Kokyuroku **1274** (2002), 62-69.

[7] Hasse, H. : Über die Dichte der Primzahlen $p$, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ teilbarer bzw. unteilbarer Ordnung mod $p$ ist, Math. Ann. **162** (1965), 74-76.

[8] _____ : Über die Dichte der Primzahlen $p$, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw. ungerader Ordnung mod $p$ ist, Math. Ann. **166** (1966), 19-23.

[9] Murata, L. and Chinen, K. : On a distribution property of the residual order of $a \pmod p$ — II, to appear in J. Number Theory.

[10] _____ : On a distribution property of the residual order of $a \pmod p$ — III in *Diophantine Problems and Analytic Number Theory*, RIMS Kokyuroku **1319** (2003), 139-147.

[11] Odoni, R. W. K. : A conjecture of Krishnamurthy on decimal periods and some allied problems, J. Number Theory **13** (1981), 303-319.